UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/535,581	03/27/2000	Rabindranath Dutta	AUS990891US1	3807

7590   05/13/2003

BRACEWELL & PATTERSON ,LLP
INTELLECTUAL PROPERY LAW
P.O. BOX 969
AUSTIN, TX 78767-0969

EXAMINER
ELISCA, PIERRE E

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

BEFORE THE BOARD OF PATENT APPEALS

AND INTERFERENCES

Paper No. 12

Application Number: 09/535,581

Filing Date: March 27, 2000

Appellant(s): Rabindranath Dutta et al.

MAILED

MAY 13 2003

GROUP 3600

James E. Boice

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/14/2003.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The amendment after final rejection filed on 1/27/2003 has been entered.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 1-12, and 18-28 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8)   Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9)   Prior Art of Record

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal.

Claims 1-12 and 18-26 are rejected under 35 U.S.C. 103 (a). This rejection is set forth in the Office action, paper #7.

Claims 27 and 28 are rejected under 35 U.S.C. 103 (a). This rejection is set forth in the Office action, paper # 7.

5,892,904	Atkinson et al.	4/1999
6,466,670	Tsuria et al.	10/2002
6,424,728	Ammar	7/2002

(10)   Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having

ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.
Claims 1-12 and 18-26 are rejected under 35 U.S.C. 103 (a) as being Unpatentable over

Atkinson et al. (U.S. Pat. 5,892,904) in view of Tsuria et al. (U.S. pat. No. 6,466,670).

As per claims 1, 3-6 and 24 Atkinson substantially discloses a certification or signing method that

ensures the authenticity and integrity of a computer program, an executable file, or code received over a

computer network. The method is used by a publisher or distributor to sign an executable file so it can be

transmitted with confidence to a recipient over an open network like the Internet (which is seen to read as

Applicant's claimed invention wherein it is stated that a method for detecting copyright violation), comprisin

the following steps:

receiving a selectable data stream of suspected copyright infringing material "or ensuring the

authencity and integrity of a computer program" (see., abstract, col 2, lines 33-67, col 3, lines

13-40, specifically wherein it is stated that this certification of the executable file or code is confirmed

or read at the recipient's computer. The public key for the publisher's signature is obtained by

decoding or decrypting the digital certificate, please note that the process of confirming

or read at the recipient's computer is readable as the step of receiving a selectable data);

generating an electronic signature for said data stream of said suspected copyright infringing material

(see., abstract, col 3, lines 13-24, figs 3 and 4, specifically wherein it is stated that the digital

certificate or electronic signature with the certification agency public key, thereby assuring the

authenticity of the software publisher, please note that the process of generating the digital certificate

is readable as the step of generating an electronic signature);

comparing signatures (see., col 3, lines 20-24, col 6, lines 34-67, col 7, lines 1-67, col 8, lines 1-29,

specifically wherein it is stated that the digest is compared to the digest included in the publisher signature. A

match or parsing or examine or analyze between the digests confirms the integrity of the code). The steps of

displaying or visually examining said suspected copyright and examining data segments matching (see., col :

lines 58-63, applicant should duly note that the user in col 5, lines 58-63 is capable of browsing documents

and displaying the document in a window 68, and therefore, capable of visually examine the documents or

materials, and the examination or matching step is disclosed in col 3, lines 13-24, please note that the

matching process also includes examining step).

Atkinson fails to explicitly disclose Applicant's newly added limitations wherein said comparing a first

electronic signature being a distillation and a second electronic signature being a distillation , that is incapabl

of reconstructing said data stream, wherein a match of said first electronic signature with said second

electronic signature indicates a likelihood that said suspected copyright infringing material (or for each

segment).

However, Tsuria discloses an anti-piracy that includes video representation signature for computing a

forbidden signature of a forbidden video representation, communication for communicating the forbidden

signature to a playing device, and a playing device adapted to receive and play back a recorded video

representation. The playback includes a signature comparison that determines whether the computed

signature of the recorded video representation matches the signature communicated to the playing device

wherein the signature comparison also includes determining that a first signature and a second signature

match even (see., abstract, col 3, lines 26-34, col 6, lines 62-67, col 7, lines 1-28). Accordingly, it would

have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the

authenticity and integrity of a computer program of Atkinson by including the first signature and the second

signature taught by **Tsuria** because such modification would prevent the distribution of pirate copies of

material which have no legitimate distribution (see., Tsuria, col 2, lines 45-50).

As per claim 2, Atkinson discloses the claimed method of receiving said data stream of suspected

copyright infringing material from the Internet (see., col 2, lines 33-67, col 3, lines 13-40, specifically wherei

it is stated that this certification of the executable file or code is confirmed or read at the recipient's

computer. The public key for the publisher's signature is obtained by decoding or decrypting the digital

certificate, Fig 2A).

As per claims 7, 9, 10, 11, 12, 25 and 26 Atkinson substantially discloses a certification or signing

method that ensures the authenticity and integrity of a computer program, an executable file, or code

received over a computer network. The method is used by a publisher or distributor to sign an executable file

so it can be transmitted with confidence to a recipient over an open network like the Internet (which is seen

to read as Applicant's claimed invention wherein it is stated that a system for detecting copyright violation),

comprising:

receiving means a selectable data stream of suspected copyright infringing material "or ensuring the

authencity and integrity of a computer program" (see., abstract, col 2, lines 33-67, col 3, lines

13-40, specifically wherein it is stated that this certification of the executable file or code is confirmed

or read at the recipient's computer. The public key for the publisher's signature is obtained by

decoding or decrypting the digital certificate, please note that the process of confirming or read at the

recipient's computer is readable as the step of receiving a selectable data);

signature generating means for generating an electronic signature for said data stream of said

suspected copyright infringing material (see., abstract, col 3, lines 13-24, figs 3 and 4, specifically

wherein it is stated that the digital certificate or electronic signature with the certification agency

public key, thereby assuring the authenticity of the software publisher, please note that the process

of generating the digital certificate is readable as the process of generating an electronic signature);
comparing means for comparing signatures (see., col 3, lines 20-24, col 6, lines 34-67, col 7, lines 1-67, col

8, lines 1-29, specifically wherein it is stated that the digest is compared to the digest included in the

publisher signature. A match or parse or examine or analyze between the digests confirms the integrity of the

code). The steps of displaying or visually examining said suspected copyright and examining data segments

matching (see., col 5, lines 58-63, applicant should duly note that the user in col 5, lines 58-63 is capable of

browsing documents and displaying the document in a window 68, and therefore, capable of visually examin

the documents or materials, and the examination or matching step is disclosed in col 3, lines 13-24, please

note that the matching process also includes examining process).

Atkinson fails to explicitly disclose Applicant's newly added limitations wherein said comparing a first

electronic signature being a distillation and a second electronic signature being a distillation , that is incapabl

of reconstructing said data stream, wherein a match of said of said first electronic signature with said second

electronic signature indicates a likelihood that said suspected copyright infringing material (or for each

segment).

However, Tsuria discloses an anti-piracy that includes video representation signature for computing a

forbidden signature of a forbidden video representation, communication for communicating the forbidden

signature to a playing device, and a playing device adapted to receive and play back a recorded video

representation. The playback includes a signature comparison that determines whether the computed

signature of the recorded video representation matches the signature communicated to the playing device wherein the signature comparison also includes determining that a first signature and a second signature match even (see., abstract, col 3, lines 26-34, col 6, lines 62-67, col 7, lines 1-28). Accordingly, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the authenticity and integrity of a computer program of Atkinson by including the first signature and the second signature taught by **Tsuria** because such modification would prevent the distribution of pirate copies of material which have no legitimate distribution (see., Tsuria, col 2, lines 45-50).

As per claim 8, Atkinson discloses the claimed limitation means for receiving said data stream of suspected copyright infringing material from the Internet (see., col 2, lines 33-67, col 3, lines 13-40, specifically wherein it is stated that this certification of the executable file or code is confirmed or read at the recipient's computer. The public key for the publisher's signature is obtained by decoding or decrypting the digital certificate, Fig 2A).

As per claims 18, 20, 21, 22, 23, Atkinson substantially discloses a certification or signing method that ensures the authenticity and integrity of a computer program, an executable file, or code received over a computer network. The method is used by a publisher or distributor to sign an executable file so it can be transmitted with confidence to a recipient over an open network like the Internet (which is seen to read as Applicant's claimed invention wherein it is stated that a method for detecting copyright violation), comprisin the following steps:

instructions within said computer readable medium for receiving a selectable data stream of suspected

copyright infringing material "or ensuring the authencity and integrity of a computer program" (see., abstract, col 2, lines 33-67, col 3, lines 13-40, specifically wherein it is stated that this certification of the executable file or code is confirmed or read at the recipient's computer. The public key for the publisher's signature is obtained by decoding or decrypting the digital certificate, please note that the process of confirming or read at the recipient's computer is readable as the step of receiving a selectable data);

instructions within said computer readable medium for generating for generating an electronic signature for said data stream of said suspected copyright infringing material (see., abstract, col 3, lines 13-24, figs 3 and 4, specifically wherein it is stated that the digital certificate or electronic signature with the certification agency public key, thereby assuring the authenticity of the software publisher, please note that the process of generating the digital certificate is readable as the step of generating an electronic signature);

instructions within said computer readable medium for comparing means for comparing signatures (see., col 3, lines 20-24, col 6, lines 34-67, col 7, lines 1-67, col 8, lines 1-29, specifically wherein it is stated that the digest is compared to the digest included in the publisher signature. A match or parse or examine or analyze between the digests confirms the integrity of the code). The steps of displaying or visually examining said suspected copyright and examining data segments matching (see., col 5, lines 58-63, applicant should duly note that the user in col 5, lines 58-63 is capable of browsing documents and displaying the document in a window 68, and therefore, capable of visually examine the documents or materials, and the examination or matching step is disclosed in col 3, lines 13-24, please note that the matching process also includes examinin step).

Atkinson fails to explicitly disclose Applicant's newly added limitations wherein said comparing a first

electronic signature being a distillation and a second electronic signature being a distillation , that is incapabl

of reconstructing said data stream, wherein a match of said of said first electronic signature with said second

electronic signature indicates a likelihood that said suspected copyright infringing material (or for each

segment).

However, Tsuria discloses an anti-piracy that includes video representation signature for computing a

forbidden signature of a forbidden video representation, communication for communicating the forbidden

signature to a playing device, and a playing device adapted to receive and play back a recorded video

representation. The playback includes a signature comparison that determines whether the computed

signature of the recorded video representation matches the signature communicated to the playing device

wherein the signature comparison also includes determining that a first signature and a second signature

match even (see., abstract, col 3, lines 26-34, col 6, lines 62-67, col 7, lines 1-28). Accordingly, it would

have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the

authenticity and integrity of a computer program of Atkinson by including the first signature and the second

signature taught by **Tsuria** because such modification would prevent the distribution of pirate copies of

material which has no legitimate distribution (see., Tsuria, col 2, lines 45-50).

    As per claim 19, Atkinson discloses the claimed method of receiving said data stream of suspected

copyright infringing material from the Internet, and instructions within said computer readable medium (see.,

col 2, lines 33-67, col 3, lines 13-40, specifically wherein it is stated that this certification of the executable

file or code is confirmed or read at the recipient's computer. The public key for the publisher's signature is

obtained by decoding or decrypting the digital certificate, Fig 2A).

Claims 27 and 28 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Atkinson et

al. (U.S. pat. No. 5,892,904) in view of Tsuria et al. (U.S. Pat. No. 6,466,670) as applied to claims 1, 5, 7, 9,

10 and 12 above, and further in view of Ammar (U.S. Pat. No. 6,424,728).

As per claim 27, Atkinson and Tsuria disclose the claimed method as stated in claims 1 and 5

above. It is to be noted that Atkinson and Tsuria fail to disclose that matching of said signatures exceeding a

predetermined number of occurrences (or signature exceeds a natural range).

However, Ammar discloses an automatic signature verification that utilizes a main routine for comparing

signatures. A dissimilarity measurements give the distance relationship of selected features of target

signature. If the dissimilarity measure of the target signature exceeds a natural range, the target signature is

judged (see., Ammar, col 1, lines 39-50, col 4, lines 65-67, col 5, lines 1-15). Therefore, it would have been

obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of

Atkinson and Tsuria by including the automatic signature verification taught by **Ammar** because such

modification would provide the required information for comparing two genuine signatures based on a

predetermined range.

As per claim 28, Atkinson and Tsuria disclose the claimed limitations as stated in claims 7, 9, 10, and 12 above. It is to be noted that Atkinson and Tsuria fail to disclose that matching of said signatures exceeding a predetermined number of occurrences (or signature exceeds a natural range). However, Ammar discloses an automatic signature verification that utilizes a main routine for comparing signatures. A dissimilarity measurements give the distance relationship of selected features of target signature. If the dissimilarity measure of the target signature exceeds his natural range, the target signature is judge (see., Ammar, col 1, lines 39-50, col 4, lines 65-67, col 5, lines 1-15). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Atkinson and Tsuria by including the automatic signature verification taught by Ammar because such modification would provide the required information for comparing two genuine signatures based on a predetermined range.

(11) RESPONSE TO ARGUMENT

In response to Applicant arguments, Applicant argues that Atkinson does not teach or suggest :

a. "a method of identifying suspected copyright infringing material and receiving streamed data segments . As specified by the Examiner in the Office action mailed on 7/16/2002, paper #3, this limitation is disclosed by Atkinson in col 2, lines 53-67, specifically wherein it is stated that the publisher digital signature also includes an identifying name of the executable file and a link or hyperlink to a description of the executable file. A publisher digital certificate is attached to the publisher signature. The publisher digital certificate is issued by a certification authority or agency to authenticate the identity of the publisher issuing the publisher signature. Applicant should duly note that this process is to identify the right signature before transmitting the file or

copyright material. The step of receiving streamed data is disclosed in col 2, lines 33-67, col 3, lines 13-40, specifically wherein it is stated that this certification of the executable file or code is confirmed or read at the recipient's computer. The public key for the publisher's signature is obtained by decoding or decrypting the digital certificate, or parsing, please note that the process of confirming or read at the recipient's computer is readable as the step of receiving a selectable data.

b. " comparing electronic signatures for different data". As specified by the Examiner in the Office action mailed on 7/16/2002, this limitation is disclosed in col 3, lines 20-24, col 6, lines 34-67, col 7, lines 1-67, col 8, lines 1-29, specifically wherein it is stated that the digest is compared to the digest included in the publisher signature. A match or a comparison between the digests confirms the integrity of the code).

c. "Virtually examining". As specified by the Examiner in the Office action mailed on 7/16/2002, this limitation is disclosed by Atkinson in col 3, lines 20-24, col 6, lines 34-67, col 7, lines 1-67, col 8, lines 1-29, specifically wherein it is stated that the digest is compared to the digest included in the publisher signature. A match between the digests confirms the integrity of the code). The steps of displaying or visually examining said suspected copyright and examining data segments matching (see., col 5, lines 58-63, applicant should duly note that the user in col 5, lines 58-63 is capable of browsing documents and displaying the document in a window 68, and therefore, capable of visually examine the documents or materials, and the examination or matching step is disclosed in col 3, lines 13-24, please note that the matching process also includes examining step).
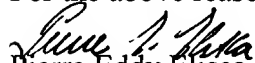
d. "Parsing said streamed data of suspected copyright material". However, the Examiner respectfully disagrees because this limitation is disclosed by Atkinson in col 3, lines 20-24, col 6, lines 34-67, col 7, lines 1-67, col 8, lines 1-29, specifically wherein it is stated that the digest is compared to the digest included in the publisher signature. A match or parsing or examine or analyze between the digests confirms the integrity of the code). The

steps of displaying or visually examining said suspected copyright and examining data segments matching (see., col 5, lines 58-63, applicant should duly note that the user in col 5, lines 58-63 is capable of browsing documents and displaying the document in a window 68, and therefore, capable of visually examine the documents or materials, and the examination or matching step is disclosed in col 3, lines 13-24, please note that the matching process also includes examining step).

e. " a first electronic signature and a second electronic signature or two signatures". However, the Examiner respectfully disagrees because this limitation is disclosed by Tsuria in col 3, lines 26-34, col 6, lines 62-67, col 7, lines 1-28, specifically wherein it is stated that an anti-piracy that includes video representation signature for computing a forbidden signature of a forbidden video representation, communication for communicating the forbidden signature to a playing device, and a playing device adapted to receive and play back a recorded video representation. The playback includes a signature comparison that determines whether the computed signature of the recorded video representation matches the signature communicated to the playing device wherein the signature comparison also includes determining that a first signature and a second signature match even (see., abstract,).

For the above reasons, it is believed that the rejections should be sustained.

Pierre Eddy Elisca

Patent examiner 5/6/2003

Bracewell & patterson, L.L.P.

111 Congress Avenue, Suite 2300

Austin, Texas 78701-4061

Respectfully submitted,

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

STEPHEN GRAVINI
PRIMARY EXAMINER

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600